

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM DADOS DE TERCEIROS

Autor:	José Damico - jose.damico@scicrop.com
Última atualização:	27/maio/2022
Revisão:	1

**PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM DADOS DE
TERCEIROS****Índice**

Contexto:	3
Objetivo	4
Termos e Expressões	5
Atores e Responsabilidades	6
Etapas Macros do Processo	7
Identificação	7
Preparação	7
Contenção	8
Erradicação	8
Recuperação	8
Lições aprendidas	8
Documentação do Incidente	8
Comunicações	9
Detalhamento do Processo	9
Início/Deteccção	9
Triagem	9
Avaliação	10
Contenção, Erradicação e Recuperação	11
Comunicações	11
Preceitos assimilados	11
Documentação	12
Observações complementares	12
Fluxo do Processo	15
Referências	16

Contexto:

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, tem como um de seus pilares centrais a implementação de medidas de Segurança da Informação que podem trazer às entidades públicas e privadas, uma cultura de maior conscientização na área. A LGPD considera que, mais grave do que sofrer um ataque ou passar por um vazamento de dados, é não se prevenir e nem adotar as medidas e práticas necessárias e possíveis para a proteção dos seus dados e de todos os que são afetados por eventuais acessos não autorizados.

A atividade de adequação às regras da Lei Geral de Proteção de Dados não se resume ao emprego de medidas tecnológicas e padrões de segurança. Inclui, também, a necessidade de elaboração, manutenção e revisão de documentos que, além de garantir a adequação à citada Lei, também são medidas que podem trazer maior organização e otimização aos processos internos, bem como, proteger a SCICROP e sua reputação, seus colaboradores, usuários dos serviços prestados, clientes e parceiros.

Atualmente, com a popularização dos computadores pessoais e a facilidade do acesso à internet, cada vez mais se observa a dependência de processos digitais para a manutenção de modelos de negócios ou cumprimento de obrigações legais. A praticidade, redução de custos e economia de tempo, advindas da informatização dos processos, traz consigo riscos de segurança que não devem ser negligenciados. Com tempo e recursos suficientes, qualquer sistema pode ser comprometido.

Levando isso em consideração, a criação de estratégias e planos para controle de danos é essencial, e é aí que entram os **Planos de Respostas a Incidentes de Segurança em Dados de Terceiros**.

Incidente de segurança é “uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados de terceiros transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento”.

Resposta a Incidentes é o processo que descreve como uma organização deverá lidar com um incidente de segurança, seja ele um ataque cibernético, uma violação de dados, a presença de um aplicativo malicioso (como um vírus), uma violação das políticas e padrões de segurança da SCICROP, dentre outros. O objetivo é minimizar os danos que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

O Plano de Respostas a Incidentes (PRI) consiste de um documento interno que deve ser amplamente conhecido por todos os colaboradores e que dispõe sobre as medidas que devem ser adotadas no caso de um Incidente de Segurança em Dados de Terceiros.

Objetivo

O Plano em questão, tem o objetivo geral de orientar a SCICROP a responder às situações de emergência e exceção, de forma documentada, formalizada, ágil e confiável, além de resguardar as evidências que possam auxiliar na prevenção de novos incidentes e no atendimento às exigências legais de comunicação e transparência.

Neste PRI serão estabelecidas funções e responsabilidades individuais e de equipes, bem como, as medidas a serem adotadas para que a SCICROP responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas/processos, proteção de informações e privacidade dos seus titulares, possibilitando manter a confiabilidade dos serviços prestados.

O presente PRI se aplica em qualquer caso de incidentes envolvendo Dados de Terceiros e deverá ser observado em conjunto com as demais políticas da empresa por todas as áreas, colaboradores e prestadores de serviços que possam vir a ter acesso às informações, arquivos e dados sob a responsabilidade da SCICROP.

O PRI SCICROP entrará em vigor na data de sua publicação, por tempo indeterminado, podendo ser revisto e alterado sempre que identificada a necessidade.

Termos e Expressões

- **Agentes de tratamento**: corresponde ao controlador e operador em conjunto. Não são considerados controladores ou operadores os colaboradores ou as equipes de trabalho de uma entidade, já que atuam sob o poder diretivo do agente de tratamento;
- **Anonimização**: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- **Ataque**: evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
- **Autoridade Nacional de Proteção de Dados - ANPD**: é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território nacional;
- **Controlador**: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;
- **Dados pessoais**: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, ou para entrar em contato, por conta própria ou quando combinada com outras informações;
- **Dados pessoais sensíveis**: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e informações bancárias;
- **Dados de terceiros**: qualquer informação privada de clientes ou parceiros da SCICROP que trafegue dentro de sistemas, software, APIs ou infraestrutura de armazenamento de dados de responsabilidade da SCICROP;
- **Encarregado ou Data Protection Officer (DPO)**: é pessoa física designada pelo controlador, responsável por assegurar o cumprimento da legislação local aplicável e atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **GT LGPD SCICROP**: Grupo de Trabalho instituído pela Portaria P nº 55/2020, com o objetivo de promover a implementação das disposições da Lei nº 13.709/2018 – LGPD);

- **Incidente**: qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da SCICROP ou que ela venha a ter acesso;
- **IP**: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;
- **LGPD**: acrônimo utilizado para identificação da Lei Geral de Proteção de Dados, a Lei nº 13.709/2018, que regula as atividades de Tratamento de Dados no Brasil.
- **Log ou Registro de eventos**: processo de registro de eventos relevantes num sistema computacional;
- **Operador**: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador. O operador será sempre uma pessoa distinta do controlador;
- **Sistemas**: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela SCICROP para dar suporte na execução de suas atividades.
- **Tratamento**: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;
- **Vazamento de dados**: qualquer quebra de sigilo ou disseminação de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;
- **Violação de privacidade**: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.
- **Vírus**: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Atores e Responsabilidades

Cada área da SCICROP possui responsabilidades quando da ocorrência ou mera suspeita de um Incidente, devendo comunicar, imediatamente, o fato ao Time de Resposta da SCICROP.

- **Notificador**: pessoa ou sistema de monitoração que notifica o incidente;

- Acionador: responsável pelo recebimento das notificações e realização do tratamento inicial (triagem) do incidente;
- Time de Resposta a Incidentes (TRI): grupo de colaboradores da SCICROP, com acessos, habilidades, responsabilidades, treinamento e conhecimentos para responder aos mais variados tipos de incidentes. O TRI será designado de acordo com as especificidades de cada incidente, sendo composto pelo Encarregado Dados (DPO) e por colaboradores de outras áreas que detenham expertise para a abordagem do tema ou cujos processos tenham sido afetados pelo incidente.
- Responsável por Sistema: indicado, com capacidade de propor soluções de resposta, bem como, autorizar ou vetar procedimentos de emergência;
- Responsável por Processo ou Negócio: responsável de uma área identificada na estrutura organizacional, com capacidade de propor soluções de resposta a serem apreciadas pelo TRI;
- GT LGPD SCICROP: principal instância decisória sobre o tratamento de Dados Pessoais no âmbito da SCICROP. Responde diretamente à Diretoria da SCICROP.

Etapas Macros do Processo

Este Plano de Resposta a Incidentes está estruturado conforme as etapas macro a seguir descritas.

Identificação

A identificação de qualquer Incidente de Segurança é aspecto chave para a boa implementação de um Plano de Respostas. É importante que se possa dispor das principais medidas de detecção e identificação de Incidentes, como ferramentas de monitoramento, registros de log, mensagens de erro de firewalls e outros sistemas de segurança, etc. Também deve haver um trabalho maciço de sensibilização e capacitação de colaboradores, para que, proativamente, esses tenham a capacidade de identificar e informar eventual vazamento de dados, de que tenham conhecimento/acesso.

Preparação

Uma resposta a um incidente deve ser decisiva e executada prontamente. Como há pouco espaço e tempo para equívocos, é essencial que as práticas de emergência sejam exercitadas e os tempos de resposta medidos. Desta forma, é possível desenvolver uma metodologia que estimule a agilidade e a exatidão, minimizando o impacto da

indisponibilidade de recursos e os potenciais danos causados pelo comprometimento do sistema/processos.

Contenção

Após a identificação de um incidente, o mesmo deve ser contido e, se for o caso, isolado, para que outros sistemas/processos não sejam afetados, evitando maiores danos ao ambiente. Essa etapa inclui a contenção de curto prazo, *backup* do sistema, contenção a longo prazo, dentre outros.

É importante que, durante a etapa de contenção, ocorra simultaneamente a adoção de medidas que permitam a documentação e o registro do incidente, devendo ser evitado que evidências e provas do ocorrido sejam destruídas ou perdidas.

Erradicação

Após a contenção da ameaça, a próxima etapa consiste na remoção da ameaça e restauração dos sistemas/processos afetados para que retornem ao seu estado original antes do incidente.

Recuperação

Nesta etapa, os sistemas/processos afetados retornarão, após testes e validações, ao ambiente de produção, ou, ao habitual andamento, com vistas a garantir que nenhuma ameaça permaneça.

Lições aprendidas

Esta última etapa visa atualizar o Plano de Respostas a Incidentes com as ações realizadas para tratar o incidente, contribuindo para o aprendizado da equipe e facilitando as próximas atuações em futuros incidentes, bem como a atualização deste documento.

Documentação do Incidente

O incidente deve ser documentado de forma detalhada, incluindo todas as ações implementadas nas etapas anteriores e as lições aprendidas com o caso.

Comunicações

A ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, deve ser comunicada à Autoridade Nacional de Proteção de Dados – ANPD e ao titular afetado. A depender da situação, as informações a serem prestadas à ANPD poderá ocorrer por meio de solicitações ou comunicações, com a finalidade principal de demonstrar, para o órgão fiscalizador, a adequação (ou intenção de adequação) da SCICROP aos ditames da lei.

Detalhamento do Processo

Início/Deteção

1. Um novo incidente é notificado por pessoa interna/externa à SCICROP ou por eventual alarme da monitoração. A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, telefone, “Fale Conosco”, Disk Denúncia, Sistemas internos (incluindo as recebidas pelo Encarregado quando se tratar de notificação do titular dos dados pessoais), devendo todas serem registradas, diretamente pelo Notificador.

Triagem

2. A Notificação é recebida pelo Acionador (Encarregado de Dados da SCICROP), que deverá fazer a avaliação preliminar ou indicar a necessidade de composição de um Time de Resposta a Incidentes (TRI) para realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes. Se for desnecessária a composição do TRI, o Acionador (Encarregado de Dados) assumirá as fases descritas no fluxo do processo que seriam de responsabilidade do TRI.
3. Na avaliação preliminar, devem ser buscadas informações sobre os sistemas/processos que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.
4. Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para trâmites regulares dentro da própria SCICROP.

Avaliação

- Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente pelo DPO/TRI, classificando-o e definindo a sua criticidade.
- A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

Volume de Dados Pessoais / Terceiros expostos	Alto	Alta Gravidade	Alta Gravidade	Alta Gravidade
	Médio	Média Gravidade	Alta Gravidade	Alta Gravidade
	Baixo	Baixa Gravidade	Média Gravidade	Média Gravidade
		Baixa	Média	Alta
Sensibilidade dos Dados Pessoais / Terceiros afetados				

Volume de Dados Pessoais / Terceiros expostos	
Criticidade	Descrição
Alto	Volume de Dados Pessoais / Terceiros afetado superior a 10% da base de dados da SCICROP.
Médio	Volume de Dados Pessoais Terceiros afetado inferior a 10% e superior a 2% da base de dados da SCICROP.
Baixo	Volume de Dados Pessoais / Terceiros afetado inferior a 2% da base de dados da SCICROP.

Sensibilidade dos Dados Pessoais / Terceiros afetados	
Criticidade	Descrição
Alta	Dados Pessoais / Terceiros de crianças/ adolescentes, dados Pessoais / Terceiros Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais / Terceiros imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências).
Baixa	Dados anonimizados, Dados Pessoais / Terceiros pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP)

- Deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos setores afetados para colaborar e isso deve ser feito a critério do DPO/TRI a qualquer momento que julgar adequado e viável.

Contenção, Erradicação e Recuperação

8. Os responsáveis pelos sistemas/processos impactados, devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção e erradicação.
9. O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades específicas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.
10. Em caso de incidente envolvendo máquinas virtuais, deve ser feito *snapshot* (registro do estado de um arquivo, aplicação ou sistema em um certo ponto no tempo) para posterior análise.
11. Em se tratando de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.
12. A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema/processo.
13. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, ou elaboração de novas rotinas processuais.

Comunicações

14. Assim que possível, a situação deve ser encaminhada para análise do GT LGPD SCICROP para avaliar se houve risco ou dano relevante aos titulares dos dados pessoais / terceiros impactados.
15. Caso o GT LGPD SCICROP conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais / terceiros, o Encarregado de Dados (DPO), deverá fazer as comunicações obrigatórias por Lei. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados e imprensa, bem como relatórios formais para a ANPD (se aplicável).

Preceitos assimilados

16. Com o incidente contido e sua resolução encaminhada, o ADPO/TRI deve agendar e conduzir uma reunião de lições aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos - inclusive deste Plano de Resposta a Incidentes.

17. As melhorias sugeridas na reunião devem ser encaminhadas ao GT LGPD SCICROP para deliberação sobre a adoção.

Documentação

18. O DPO/TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações executadas, inclusive as da reunião de lições aprendidas.
19. Após a neutralização da ameaça, o Encarregado de Dados (DPO) deve elaborar um relatório circunstanciado de todas as medidas que foram adotadas, apresentando todas as informações relevantes, tais como, informações sobre o incidente em si (quando foi identificado, qual sua natureza, danos ou potenciais danos causados, a extensão, a relevância e a repercussão desses danos, etc); providências adotadas para preservação das evidências, procedimentos seguidos para a contenção da crise; medidas de correção técnicas e de Governança adotadas; questionamentos e demandas externas (requerimentos de titulares de dados, autoridades e imprensa, bem como suas respostas - se aplicável); deliberações do TRI e do GT LGPD SCICROP.

Observações complementares

Paralelamente à execução do Plano de Respostas a Incidentes, diversas ações devem ser desenvolvidas, antes, durante e depois da ocorrência de um incidente, conforme:

Durante o incidente - Identificação, coleta e preservação das evidências:

Como já mencionado, um aspecto essencial da Resposta aos Incidentes é a coleta e preservação de evidências que possam vir a ser úteis ou necessárias para a SCICROP, por exemplo, para demonstrar às autoridades (se aplicável) que houve uma resposta adequada e que o incidente foi tratado com a seriedade necessária.

Especialmente no contexto da LGPD e da ANPD, as providências adotadas pela SCICROP, para conter o Incidente e seus danos, podem ser definitivas para a minimização das sanções e multas, eventualmente, aplicadas ao caso concreto e tão somente, se aplicáveis por lei. Tais evidências também se prestam a possibilitar a identificação/responsabilização do usuário causador do vazamento de dados pessoais / terceiros. Diversas decisões na União Europeia, em decorrência da GDPR (General Data Protection Regulation ou Regulamentação Geral de Proteção de Dados da União Europeia), demonstram que, mais grave do que o incidente em si, é o fato de a organização desprezá-lo.

Após o incidente - Elaboração de relatório final do incidente e revisão dos procedimentos:

O relatório, além de ter uma função de comprovação das medidas levadas a efeito pela SCICROP, é importante para que se possa compreender as causas do incidente, avaliar a aderência e efetividade do Plano de Respostas a Incidentes e analisar a atuação dos responsáveis.

No que tange à Comunicação de Incidente de Segurança, prevista na LGPD, cujo conteúdo mínimo está definido no artigo 48, temos:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

I – a descrição da natureza dos dados pessoais afetados;

Não basta apontar se os dados pessoais / terceiros são convencionais (art. 5º, I) ou sensíveis (art. 5º, II), mas deve-se arrolar, com precisão, as espécies: contas de e-mail, dados de cartão de crédito, senhas, informações de geolocalização, etc., para que o titular tenha uma ideia, ainda que estimada, dos riscos existentes ou dos danos possíveis.

II – as informações sobre os titulares envolvidos;

É a descrição, precisa ou estimada, de quais e quantos titulares foram afetados.

III – a indicação das medidas técnicas e de segurança utilizadas para a proteção;

Observados os segredos comercial e industrial, a LGPD exige, em seu art. 46, que os agentes de tratamento (controlador e operador) adotem medidas de segurança (técnicas e administrativas) para a proteção de dados pessoais / terceiros. Tais medidas devem ser descritas, para demonstrar a aderência com a lei. Obviamente, essa descrição minuciosa admite algumas limitações, como os segredos comercial e industrial, que devem ser poupados para a preservação do negócio. A depender do tipo de incidente e, em havendo o risco de ser repetido, a descrição de determinadas medidas de segurança adotadas também poderia ser ocultada, segundo a técnica da “segurança por obscuridade” (*Security Through Obscurity – STO*), que teria o condão de privar o adversário/atacante de qualquer informação que possa ajudá-lo a comprometer a organização.

IV – os riscos relacionados ao incidente;

Trata-se de uma análise prospectiva do incidente, levando em consideração, principalmente, os itens I e II. Poderá mencionar, também, os danos que já ocorreram, como a destruição ou codificação de dados.

V – os motivos da demora, no caso de a comunicação não ter sido imediata;

É a justificativa, devidamente fundamentada, da não apresentação imediata da notificação. Poderá decorrer, por exemplo, da complexidade e extensão (número de titulares afetados, quantidade de dados, etc.) do incidente.

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

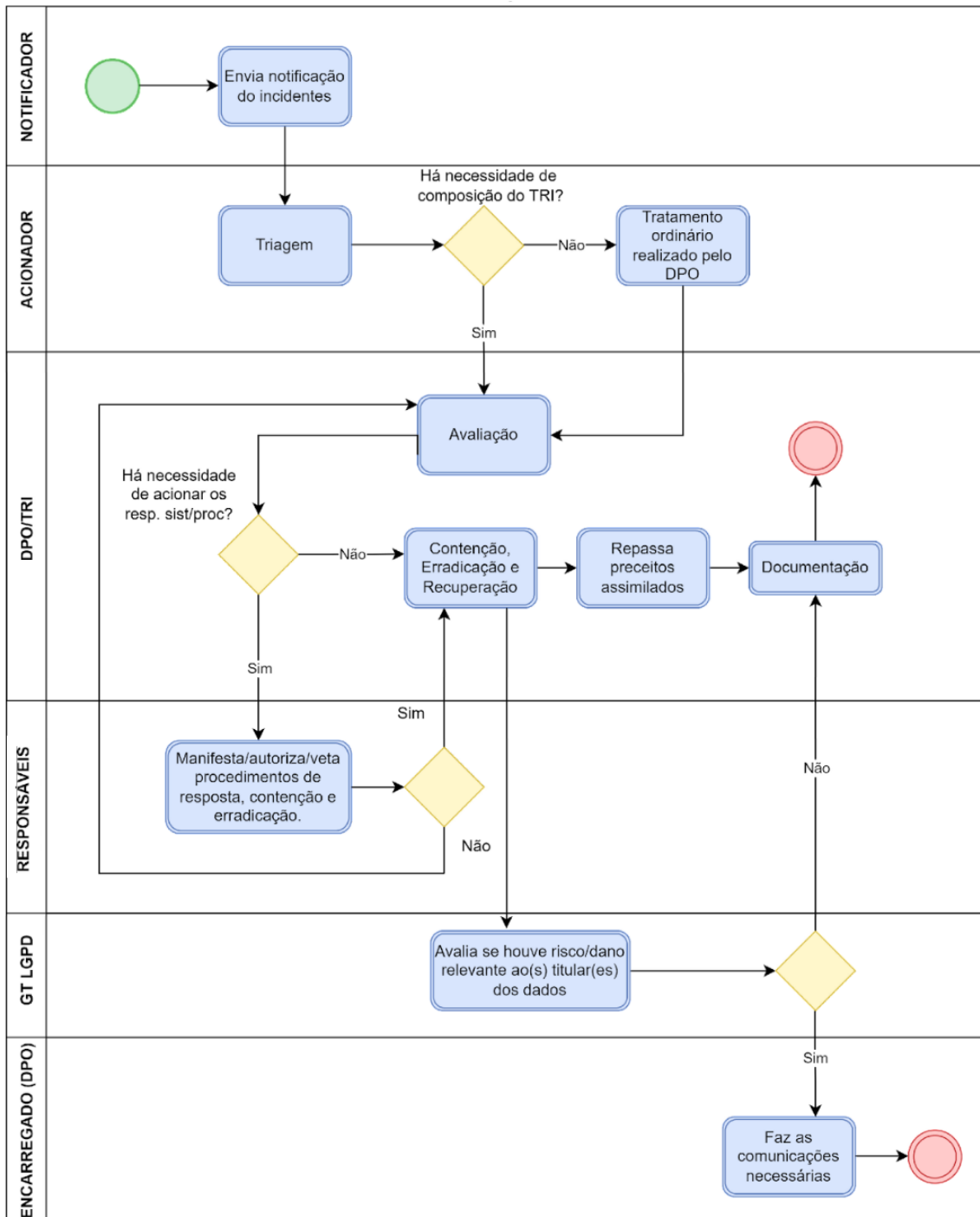


SCICROP INFORMAÇÃO E TECNOLOGIA S.A.

CNPJ: 23.587.791/0001-01

Aqui devem ser mencionadas, de forma clara e objetiva, e sem exagero de expressões técnicas, as condutas que foram e que serão implementadas para eliminar ou minimizar os efeitos do incidente, como o contato com as autoridades policiais, determinação de troca de senhas pelos usuários, a atualização de sistemas e servidores, etc.

Fluxo do Processo



Referências

- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentosexternos/anpd_guia_agentes_de_tratamento.pdf>.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/Ato2015-2018/2018/Lei/L13709.htm>.